SOPHOS
Cybersecurity delivered.

ZT Sophos Zero Trust Network

Sophos ZTNA Qualification Guide

Zero Trust Network Access is the ultimate remote-access VPN replacement

Who is the Buyer?

The decision maker for ZTNA will often be the desktop IT administrator who's responsible for ensuring his remote workers have the tools they need to do their job. It may also involve the network buyer who will likely be pleased to hear that remote-access VPN is not longer required.

Conversation Starter, Prospecting Script, Elevator Pitch:

Do you have remote workers or an interest in implementing zero trust? How are you addressing the challenges with a remote workforce and properly securing your networked applications?

- Many organizations such as yours are grappling with the challenges of supporting a remote workforce and the issues that accompany remote-access VPN and access to the applications they need to do their jobs.
- Fortunately, there's a better way to do remote access now – ZTNA. Zero Trust Network Access is a lot easier, more scalable, more transparent for end users, doesn't have performance issues, works anywhere and everywhere, and provides better protection from Ransomware and other threats.
- And with Sophos ZTNA, it deploys in a single agent with Sophos Intercept X providing the best endpoint protection and ZTNA in a single agent, all managed from a single console, from a single vendor – making your life a lot simpler and easier. It's a unique solution you won't find anywhere else.

Why ZTNA?

More Controlled Access

VPN provides broad network access, ZTNA provide specific app access this micro-segmentation reduces risk and the ability for threats to move laterally.

Enhanced Security

ZTNA eliminates old vulnerable VPN clients, integrates device health into policy, and eliminates lateral movement.

Works Anywhere

ZTNA will work on any network (home, hotel, airport) and even within the corporate network without issues that commonly plague VPN.

Transparent

ZTNA is much more transparent for end-users – it "just works".

Better Visibility

With VPN, admins have no idea what users are doing while ZTNA provides granular insights into application usage.

Easer Management

Cloud managed ZTNA is much more scalable and easier to add and decommission users and apps than firewall managed VPN.

Why Sophos ZTNA?

Sophos ZTNA offers a unique Single Agent, Single Console, Single Vendor solution which means much easier deployment, less footprint on the device, easier management and integration with other Sophos Products for Synchronized Security and simple licensing and lower TCO.

Qualification Guide

Your Prospect is a fit for Sophos ZTNA if they answer "Yes" to the following questions:

Does the Prospect have...	Yes...
... remote workers or an interest in zero trust?	ZTNA is an ideal fit for remote workers and building a zero trust network
... their own hosted applications?	ZTNA is an ideal way to provide secure access to these applications – Note ZTNA is not designed to control access to SaaS apps
... hosted applications on-premise or in AWS?	Sophos ZTNA can provide secure access to these applications with other public cloud platforms coming soon
... uses Active Directory (on prem or in Azure) or Okta?	Sophos ZTNA works with Azure or Okta as the identity provider – with more IDP support coming soon
... VMware onsite?	Sophos ZTNA gateways run in on VMware Esxi with Hyper-V and other platforms coming soon
... Windows on the end-user's devices	Sophos ZTNA can currently provide secure access for Windows users with macOS and other client platforms coming soon
... Intercept X or are interested in Intercept X?	Sophos ZTNA is nicely integrated with Intercept X and managed in Sophos Central but also works with any endpoint product

Objection Handling:

I'm perfectly happy with my remote-access VPN solution

- This may be true if they just have a few users, but if they grow at all, it may become a significant pain.
- If they are at all concerned about Ransomware, moving from VPN to ZTNA will provide much better protection against attacks trying to exploit VPN to get on the network.

VPN access is cheap or free

- This is often true, although there are hidden costs associated with VPN – such as the time and energy spent managing it. And as with most things in life, you get what you pay for which definitely applies in this case in terms of security and protection.

We need support for platform X

- They may require a platform for clients, gateways, or identity providers we don't currently support. If that's the case, then we likely have it on our roadmap and we should stay in touch as we will likely support their required platform soon. For example, Mac client and Hyper-V gateway support is already underway.

I'm already using a ZTNA solution from vendor A

- This is great, there is no reason for them to switch unless they are considering our Sophos Intercept X for their endpoints, in which case, also switching to our ZTNA solution offers a ton of added benefits – single agent, single console, single vendor, simpler licensing, and better integrated protection with Synchronized Security.

Get more info at Sophos.com/ztna

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

SOPHOS